PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-044607
(43)Date of publication of application : 14.02.2003

(51)Int.Cl. G06F 17/60

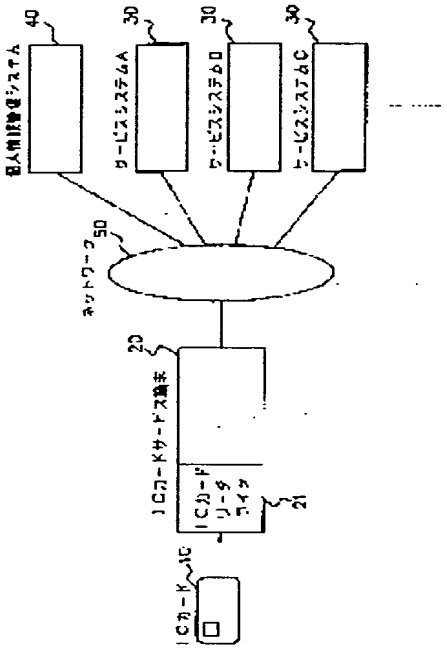
(21)Application number : 2001-273520
(22)Date of filing : 10.09.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NISHIDA GEN
TAKAKURA TAKESHI
HAYASHI RYOICHI

(30)Priority
Priority number : 2001152377 Priority date : 22.05.2001 Priority country : JP

(54) SYSTEM FOR INTEGRATED MANAGEMENT OF PERSONAL INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system for integrated management of personal information by which a user himself or herself can manage personal information on the user and which allows personal information needed by the system to be used under conditions permitted by the user.
SOLUTION: An IC card service terminal 20 having an IC card reader/writer to transmit and receive data to from an IC card 10 stored the personal information, a plurality of service systems 30 providing service to the user via the IC card 10 and the service terminal 20 by using the personal information stored in the IC card 10 and a personal information management system 40 providing service to manage the personal information of the user stored into the IC card 10 are connected via a network 50, so that a personal information management system 40 can provide the personal information to each service system 30 within the ranges permitted by each user.



LEGAL STATUS
[Date of request for examination] 13.07.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－44607
（P2003－44607A）
(43)公開日　平成15年２月14日(2003.2.14)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	テーマコード*（参考）
Ｇ０６Ｆ　17/60	１３２	Ｇ０６Ｆ　17/60	１３２
	５１０		５１０
	５１２		５１２

審査請求　未請求　請求項の数16　ＯＬ　（全 14 頁）

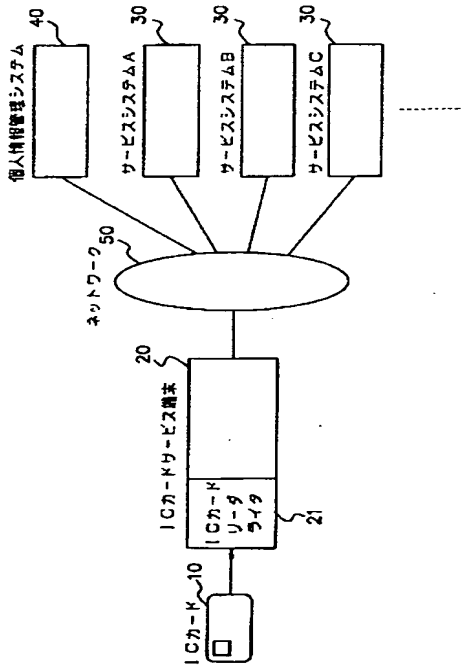
(21)出願番号　特願2001－273520(P2001－273520)
(22)出願日　平成13年９月10日(2001.9.10)
(31)優先権主張番号　特願2001－152377(P2001－152377)
(32)優先日　平成13年５月22日(2001.5.22)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　西田　玄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　▲髙▼倉　健
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100069981
弁理士　吉田　精孝

最終頁に続く

(54)【発明の名称】　個人情報統合管理システム及びそのプログラム並びにそのプログラムを記録した媒体

(57)【要約】
【課題】　ユーザの個人情報をユーザ自身が管理でき、サービスシステムが必要とする個人情報はユーザが許可した条件下でのみ利用可能となし得る個人情報統合管理システムを提供すること。
【解決手段】　個人情報を格納したＩＣカード１０との間でデータを送受信するためのＩＣカードリーダライタを有するＩＣカードサービス端末２０と、ＩＣカードに格納されたユーザの個人情報を利用し、ＩＣカード１０及びＩＣカードサービス端末２０を通じてユーザにサービスを提供する複数のサービスシステム３０と、ＩＣカード１０に格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システム４０とをネットワーク５０を介して接続することにより、個人情報管理システム４０から各サービスシステム３０へのユーザが許可した範囲での個人情報の提供を可能とする。



【特許請求の範囲】
【請求項１】　少なくともユーザの個人情報を格納したＩＣカードと、ＩＣカードとの間でデータを送受信するためのＩＣカードリーダライタを有するＩＣカードサービス端末と、ＩＣカードにＩＣカード用アプリケーションプログラムを提供するとともにＩＣカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したＩＣカード及びＩＣカードサービス端末を通じてユーザにサービスを提供する複数のＩＣカードサービスシステムと、ＩＣカードサービス端末と複数のＩＣカードサービスシステムとを接続するネットワークとからなり、
前記ＩＣカードサービスシステムとして、
ＩＣカードに格納されたユーザの個人情報を利用してユーザにサービスを提供するサービスシステムを少なくとも１つ具備し、
かつ、
ＩＣカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムを具備したことを特徴とする個人情報統合管理システム。
【請求項２】　前記ＩＣカードサービスシステムとして、前記に加え、ＩＣカードに本システムにおけるユニークなユーザＩＤを払い出す機能と、個人情報を初期入力する機能と、入力した情報を参照し、確認し、保存する機能とを有するＩＣカード登録アプリケーションを実行する個人情報登録システムを具備したことを特徴とする請求項１に記載の個人情報統合管理システム。
【請求項３】　前記ユーザの個人情報は、ユーザＩＤを含む個人を特定する又は特徴づけるための基本情報と、各サービスシステムを利用する際に使用するアプリケーション個人情報と、前記個人情報管理システム及び前記サービスシステムを利用する際に取得した個人履歴情報と、これら基本情報、アプリケーション個人情報及び個人履歴情報の各項目についての利用条件を定めた利用条件情報とからなり、
前記サービスシステムは、該サービスシステムを特定する又は特徴づけるためのサービスシステム情報と、該サービスシステムが独自に収集した該サービスシステムの利用者の顧客情報と、ＩＣカードに格納された個人情報のうちユーザが該サービスシステムに対して定めた利用条件の範囲で複製した個人情報とを格納し、
前記個人情報管理システムは、ＩＣカードに格納された個人情報のうちユーザが該個人情報管理システムに対して定めた利用条件の範囲で複製した個人情報と、サービスシステムに格納されたサービスシステム情報のうちサービスシステムが許可した範囲で複製したサービスシステム情報とを格納することを特徴とする請求項１または２に記載の個人情報統合管理システム。
【請求項４】　前記サービスシステムは、
ＩＣカードに格納された個人情報のうちユーザが該サービスシステムに対して定めた利用条件の範囲で複製した個人情報と、該サービスシステムが独自に収集した該サービスシステムの利用者の顧客情報とを格納する顧客情報データベースと、
該サービスシステムが提供するサービスをユーザの要求に応じて処理するサービス処理モジュールとにより構成されることを特徴とする請求項１または２に記載の個人情報統合管理システム。
【請求項５】　前記ＩＣカードサービス端末は、ユーザの要求に基づき該ユーザがサービスシステムを利用した時の個人履歴情報をＩＣカードに送信する機能を有し、前記ＩＣカードは、ＩＣカードサービス端末から送信された個人履歴情報を蓄積する機能を有することを特徴とする請求項１または２に記載の個人情報統合管理システム。
【請求項６】　前記ＩＣカードは、ＩＣカードサービス端末から送信されたサービスシステム毎にフォーマットが異なるサービス利用時の個人履歴情報を、統一されたフォーマットの個人履歴情報に変換する機能を有することを特徴とする請求項５に記載の個人情報統合管理システム。
【請求項７】　前記個人情報管理システムは、
ＩＣカードに格納された個人情報のうちユーザが該個人情報管理システムに対して定めた利用条件の範囲で複製した個人情報を格納する個人情報データベースと、
サービスシステムに格納されたサービスシステム情報のうちサービスシステムが個人情報管理システムに対して定めた利用条件の範囲で複製したサービスシステム情報を格納するサービスシステムデータベースと、
個人情報管理システムにアクセスするユーザの認証と、アクセス対象となった個人情報の利用条件情報の解析と、ユーザの個人情報操作内容を解釈し該操作が意味する個人情報管理サービスの実行とを行う個人情報管理モジュールと、
個人情報管理システムにアクセスするサービスシステムの認証と、アクセス対象個人情報の利用条件情報の解析と、サービスシステムが個人情報管理システムに要求する処理内容の判断とを行うサービスシステム管理モジュールと、
個人情報管理モジュールやサービスシステム管理モジュールにおける、個人情報データベースやサービスシステムデータベースから読み出した情報を処理し、個人情報管理システム外部に出力する際に該情報に対する利用条件を設定し、該利用条件情報に基づき利用制御する利用制御モジュールとにより構成されることを特徴とする請求項１または２に記載の個人情報統合管理システム。
【請求項８】　前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、

結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有することを特徴とする請求項１乃至７のいずれかに記載の個人情報統合管理システム。

【請求項９】　顧客情報と個人情報との関連付けを行う前記情報連携機能は、サービスシステムに対し匿名性を維持して処理することを特徴とする請求項８に記載の個人情報統合管理システム。

【請求項１０】　前記情報連携機能は、

ＩＣカードに格納された個人情報を、ユーザＩＤを含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、

ＩＣカードまたは個人情報管理システムにおいて暗号鍵と復号鍵と鍵ＩＤとを作成し、暗号鍵と鍵ＩＤをＩＣカードに格納し、復号鍵と鍵ＩＤを個人情報管理システムの復号鍵データベースに格納する第二の事前処理ステップと、

ＩＣカードにおいてユーザＩＤを第二の事前処理ステップで得た暗号鍵で暗号化した暗号化ユーザＩＤを生成して格納する第三の事前処理ステップと、

ＩＣカードからサービスシステムに暗号化ユーザＩＤと鍵ＩＤを送信するサービス利用ステップと、

サービスシステムから個人情報管理システムに顧客情報と暗号化ユーザＩＤと鍵ＩＤとを送信する第一の連携処理ステップと、

個人情報管理システムにおいて鍵ＩＤを用いて復号鍵データベースから該鍵ＩＤに対応する復号鍵を検索し、該復号鍵で暗号化ユーザＩＤを復号してユーザＩＤを特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザＩＤを用いて個人情報データベースから該ユーザＩＤに対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって実現されることを特徴とする請求項８または９に記載の個人情報統合管理システム。

【請求項１１】　少なくともユーザの個人情報を格納したＩＣカードと、ＩＣカードとの間でデータを送受信するためのＩＣカードリーダライタを有するＩＣカードサービス端末と、ＩＣカードにＩＣカード用アプリケーションプログラムを提供するとともにＩＣカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したＩＣカード及びＩＣカードサービス端末を通じてユーザにサービスを提供する複数のＩＣカードサービスシステムと、ＩＣカードサービス端末と複数のＩＣカードサービスシステムとを接続するネットワークとからなり、

前記ＩＣカードサービスシステムとして、

ＩＣカードに格納されたユーザの個人情報を利用してユーザにサービスを提供するサービスシステムを少なくとも１つ具備し、

かつ、

ＩＣカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムを具備した個人情報統合管理システムのプログラムであって、該プログラムはコンピュータ上に、

ＩＣカードに格納された個人情報のうちユーザが該サービスシステムに対して定めた利用条件の範囲で複製した個人情報と、該サービスシステムが独自に収集した該サービスシステムの利用者の顧客情報とを格納する顧客情報データベースと、

該サービスシステムが提供するサービスをユーザの要求に応じて処理するサービス処理モジュールとにより構成されるサービスシステムを実現することを特徴とする個人情報統合管理システムのプログラム。

【請求項１２】　少なくともユーザの個人情報を格納したＩＣカードと、ＩＣカードとの間でデータを送受信するためのＩＣカードリーダライタを有するＩＣカードサービス端末と、ＩＣカードにＩＣカード用アプリケーションプログラムを提供するとともにＩＣカードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動したＩＣカード及びＩＣカードサービス端末を通じてユーザにサービスを提供する複数のＩＣカードサービスシステムと、ＩＣカードサービス端末と複数のＩＣカードサービスシステムとを接続するネットワークとからなり、

前記ＩＣカードサービスシステムとして、

ＩＣカードに格納されたユーザの個人情報を利用してユーザにサービスを提供するサービスシステムを少なくとも１つ具備し、

かつ、

ＩＣカードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムを具備した個人情報統合管理システムのプログラムであって、該プログラムはコンピュータ上に、

ＩＣカードに格納された個人情報のうちユーザが該個人情報管理システムに対して定めた利用条件の範囲で複製した個人情報を格納する個人情報データベースと、

サービスシステムに格納されたサービスシステム情報のうちサービスシステムが個人情報管理システムに対して定めた利用条件の範囲で複製したサービスシステム情報を格納するサービスシステムデータベースと、

個人情報管理システムにアクセスするユーザの認証と、アクセス対象となった個人情報の利用条件情報の解析と、ユーザの個人情報操作内容を解釈し該操作が意味する個人情報管理サービスの実行とを行う個人情報管理モジュールと、

個人情報管理システムにアクセスするサービスシステムの認証と、アクセス対象個人情報の利用条件情報の解析

と、サービスシステムが個人情報管理システムに要求する処理内容の判断とを行うサービスシステム管理モジュールと、
個人情報管理モジュールやサービスシステム管理モジュールにおける、個人情報データベースやサービスシステムデータベースから読み出した情報を処理し、個人情報管理システム外部に出力する際に該情報に対する利用条件を設定し、該利用条件情報に基づき利用制御する利用制御モジュールとにより構成される個人情報管理システムを実現することを特徴とする個人情報統合管理システムのプログラム。
【請求項１３】　前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、
結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有することを特徴とする請求項１２に記載の個人情報統合管理システムのプログラム。
【請求項１４】　顧客情報と個人情報との関連付けを行う前記情報連携機能は、サービスシステムに対し匿名性を維持して処理することを特徴とする請求項１３に記載の個人情報統合管理システムのプログラム。
【請求項１５】　前記情報連携機能は、
ＩＣカードに格納された個人情報を、ユーザＩＤを含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、
ＩＣカードまたは個人情報管理システムにおいて暗号鍵と復号鍵と鍵ＩＤとを作成し、暗号鍵と鍵ＩＤをＩＣカードに格納し、復号鍵と鍵ＩＤを個人情報管理システムの復号鍵データベースに格納する第二の事前処理ステップと、
ＩＣカードにおいてユーザＩＤを第二の事前処理ステップで得た暗号鍵で暗号化した暗号化ユーザＩＤを生成して格納する第三の事前処理ステップと、
ＩＣカードからサービスシステムに暗号化ユーザＩＤと鍵ＩＤを送信するサービス利用ステップと、
サービスシステムから個人情報管理システムに顧客情報と暗号化ユーザＩＤと鍵ＩＤとを送信する第一の連携処理ステップと、
個人情報管理システムにおいて鍵ＩＤを用いて復号鍵データベースから該鍵ＩＤに対応する復号鍵を検索し、該復号鍵で暗号化ユーザＩＤを復号してユーザＩＤを特定する第二の連携処理ステップと、
個人情報管理システムにおいてユーザＩＤを用いて個人情報データベースから該ユーザＩＤに対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって実現されることを特徴とする請求項１３または１４に記載の個人情報統合管理システムのプログラム。
【請求項１６】　請求項１１乃至１５のいずれかに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数のＩＣカードサービスシステムで使用されるユーザの個人情報を、ユーザ自身が主体的に管理し、かつＩＣカードサービスシステムに必要な個人情報の使用をユーザが設定した利用条件に基づいて制御する、個人情報統合管理システムを実現するための技術に関する。
【０００２】
【従来の技術】従来、サービスの提供者が、サービス利用履歴や趣味・嗜好等のユーザの個人情報を管理し、これをユーザに対するマーケティングに活用するケースが数多く見受けられていた。
【０００３】近年は、ＩＣカードを用いたＩＣカードサービスシステムを構築して、ユーザ情報の管理を行うシステムが増加している。これは、耐タンパ性に優れたＩＣカードの安全性を活用しようというもので、課金・決裁・資産管理サービスのような金銭の出納に関わるサービスや、電子行政・医療情報システムなど、繊細な情報やプライバシーに関わる情報を扱うサービスに対し、暗号・認証技術を用いた堅牢なユーザ認証を実現するために導入されたものである。
【０００４】ＩＣカードは、従来の磁気カードと比べ高コストであることから、複数のＩＣカードサービスシステムを１枚のカードで共用できるような高機能性が求められていたが、最近のＩＣチップの演算能力と記憶容量の向上に伴い、１枚のＩＣカードに複数のアプリケーション処理プログラムを搭載することができるようになった。これに併せ、ＩＣカードに搭載するアプリケーションについても、共通の開発環境と実行環境を提供するプラットフォームが開発されている（例えば、ＮＴＴ技術ジャーナル、２０００年１０月号、ｐ．１５－１８、ｐ５６－５９参照）。
【０００５】ＩＣカードサービスシステム開発の現状を見ると、ＩＣカード媒体の特徴である携行性と安全性を活かしたシステム構築がなされてはいるものの、ＩＣチップの演算処理能力を応用した高機能性の十分な活用には至っていないようである。
【０００６】具体的には、これまでのＩＣカードサービスシステムでは、ＩＣカードからＩＣカードサービスシステムにデータベース処理言語であるＳＱＬコマンドを送信することで、ＩＣカードサービスシステムの個人情報データベースに対する処理を実行する等、ＩＣカードに単なる情報蓄積媒体以上の機能を発揮させていた。
【０００７】しかし、ＩＣカード上での処理は、ＩＣカ

ードに蓄積されていた該ＩＣカードサービスシステム向けに用意された処理プログラムとパラメータが選択され起動されるというものであり、高機能ＩＣカードサービスシステムの使い道としては比較的容易な処理内容に過ぎなかった。

【０００８】一方、ＩＣカードサービスシステムで使用される個人情報については、上述したように、従来からマーケティングに役立つ情報として認められていたが、近年の通信ネットワークの普及に伴う電子サービスの中て、電子化された個人情報を用いることで容易に実現されるようになったマス・カスタマイゼーションが、マーケティング戦略面のみならず、効率面でも有効であることが判明すると、特に電子化された個人情報の価値はますます増大してきた。事実、通信ネットワーク上でのサービス提供企業が売却される際に、該企業の有する個人情報が重要な資産価値として認められもしている。

【０００９】しかしながら、個人情報が電子化され通信ネットワーク上で利用されることには、ユーザとして安全面での懸念がある。セキュリティ、プライバシーの問題がそれである。個人情報保護に関する法律制定の動きもあるが、ユーザも自己防衛を考えるようになり、また、サービス提供者としても信用問題につながるため、相当の力を入れるようになってきつつある。

【００１０】通信ネットワークにおける個人情報流通を技術面から支えるため、暗号・認証やデータ利用制御技術が開発され、後者においては、ユーザがユーザ自身の個人情報に利用条件を課す方法が考案されている（例えば、寺西裕一　他「利用規約に基づくマルチメディアコンテンツ流通システムの設計」情処研報９９－ＤＰＳ－９５、Ｖｏｌ．９９、Ｎｏ．９４、１９９９、ｐｐ３１－３６参照）。これは、個人情報の管理に対しユーザが主導権を持つことにつながり、また、個人情報が通信ネットワーク上を流通する世界を想定したものでもある。

【００１１】

【発明が解決しようとする課題】このような状況の下、多数のＩＣカードサービスシステム導入の動きがあるが、現状のままでＩＣカードサービスシステムの構築が進められると、ユーザの個人情報が複数のＩＣカードサービスシステムで独立に存在し、各ＩＣカードサービスシステムで管理されることになる。すると、ユーザの個人情報は各ＩＣカードサービスシステムで管理され、ＩＣカードサービスシステムの数だけ存在することになるので、ユーザは利用したいシステムの数だけＩＣカードを携帯する必要が生じ、ユーザ自身の個人情報であるにも拘わらず、ユーザ自身で管理することができず、ユーザの個人情報に何らかの変更が生じた場合、複数のシステムに対してそれぞれ個人情報更新処理を行わなければならなくなる。また、ユーザはユーザ自身の個人情報がどこでどのように使用されているか把握できず、個人情報がユーザの意図に沿わない使われ方をされる可能性がある。

【００１２】そこで、本発明では、ＩＣカードサービスシステム毎に管理されているユーザの個人情報を、ユーザ自身が管理できるようにし、各ＩＣカードサービスシステムが必要とする個人情報をユーザが許可した条件の下でのみ利用可能とし、ＩＣカードサービスシステムに提供した個人情報の使われ方を制御できる個人情報統合管理システムを提供することを目的とする。

【００１３】また、派生的課題として、ＩＣカードサービスシステム間で個人情報を流通する際に、ユーザが予想していないシステム間の情報連携により、個人のプライバシーに関わる情報が生じる危険がある。そこで、このような個人情報を生成しない、または、生成されても利用を制御可能にする技術を提供することも、本発明で解決すべき課題である。

【００１４】

【課題を解決するための手段】上記の課題を解決するために、本発明では、ＩＣカードの多機能性を従来以上に発揮させ、１枚のＩＣカードに複数のサービス処理機能を持たせてワンカード化を図り、また、暗号・認証技術と利用制御技術を利用して、個人情報の安全な流通の仕組みを設ける。そして、ＩＣカードと複数のＩＣカードサービスシステムが相互に情報連携しての処理が可能となるＩＣカードサービス環境を構築する。

【００１５】具体的には、ＩＣカード上に、個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のＩＣカードサービスシステムのＩＣカードにおける処理プログラム（カード用サービスＡＰ）及びこれに用いる情報（ＡＰ個人情報）を、複数サービス分だけ搭載する。この時、ＩＣカードサービスシステムの１つとして、ユーザの個人情報を管理するサービスを行う個人情報管理システムを用意し、該システムのＩＣカードにおける処理プログラム（カード用管理ＡＰ）をＩＣカードに搭載しておく。

【００１６】ＩＣカードサービス端末は、ユーザからの要求に基づいて、ユーザがサービスシステムを利用した時に該サービスシステムが収集した情報をＩＣカードに送信し、ＩＣカードのカード用管理ＡＰは受信したサービス利用に関する情報を、そのサービスシステム毎に異なるフォーマットを適当なフォーマットに揃えて個人履歴情報として蓄積する。

【００１７】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び通常の各ＩＣカードサービスシステム（以下、サービスシステムと略す）のＡＰ個人情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービスとして提供する。また、個人情報管理システムは、サービスシステム情報を管理する機能を有する。そして、あるサービスシステムに対する個人情報を

用いた処理においては、該サービスシステムに対応するサービスシステム情報と個人ＡＰ情報を参照することで、個人情報の利用制御や、情報連携サービスや、カード用サービスＡＰの処理制御を行う。

【００１８】一方、システム間での情報連携が個人のプライバシーを侵害するのを防ぐために、サービスシステムの顧客情報と、管理システムの個人情報を匿名のまま関連付ける仕組みを設ける。

【００１９】ユーザ個人を識別するためのユーザＩＤを暗号化した暗号化ユーザＩＤと、暗号鍵を識別する鍵ＩＤを設定し、サービスシステムに提供する個人情報に暗号化ユーザＩＤと鍵ＩＤを付加する。

【００２０】また、管理システムでは、鍵ＩＤに対応した復号鍵を検索できるように復号鍵を格納する復号鍵データベースを構築する。

【００２１】

【作用】本発明の個人情報統合管理システムは、個人情報管理サービスを提供する個人情報管理システムと、各種サービスを提供する複数のサービスシステムと、カードリーダライタが付属したＩＣカードサービス端末と、そして、各ユーザの個人情報等を蓄積したＩＣカードにより構成される。ＩＣカード上には、個人情報管理システムで管理する個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のサービスシステムのカード用サービスＡＰ及びＡＰ個人情報を搭載する。ここで、ＩＣカード上の個人情報の個人履歴情報は、サービス利用時にサービスシステムからＩＣカードサービス端末を通じて送信されるものである。

【００２２】個人情報統合管理システムでは、ＩＣカードサービスシステムの１つとして個人情報管理システムを用意し、ユーザの個人情報を管理するサービスを行う。個人情報管理サービスを利用するには、ＩＣカードサービス端末で、カード用個人情報管理ＡＰ（カード用管理ＡＰ）をＩＣカードに予めダウンロードする。そして、ユーザはＩＣカードサービス端末（カード端末）で個人情報管理サービスのクライアントプログラム（端末用管理ＡＰ）を起動する。

【００２３】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び各サービスシステムの個人ＡＰ情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービス（管理サービス）として提供する。

【００２４】ユーザが各サービスシステムのサービスを利用するには、カード端末で、利用する各サービスシステムのカード用サービスＡＰを予めＩＣカードにダウンロードする。そして、ユーザはＩＣカードサービス端末（カード端末）で利用したいサービスシステムのクライアントプログラム（端末用サービスＡＰ）を起動する。端末用サービスＡＰは、カード用管理ＡＰが管理する個人情報及び利用条件情報と、カード用サービスＡＰが管理する個人情報を利用して、各サービスシステムが提供する様々な処理を行う。

【００２５】個人情報管理システムの管理サービスは、サービスシステムの個人情報要求に対し、ユーザが設定した個人情報と利用条件情報とを用い、ユーザが許可した範囲で個人情報を提供する。ＩＣカードがシステムに接続されていない場合も、管理サービスは利用条件付き個人情報を提供できる。

【００２６】個人情報管理システムとサービスシステムとの情報連携については、サービスシステムから個人情報管理システムに情報連携処理要求があると、管理システムは適切な復号鍵を検索し、暗号化ユーザＩＤを復号してユーザＩＤを特定し、該ユーザＩＤの個人情報と関連付ける。この関連付け処理では、ユーザＩＤをシステム処理の工程内でのみ使用しているので、結果を抽出する前に利用条件に基づく利用制御を行うことで、プライバシーを侵害するような情報連携を避けることができる。

【００２７】

【発明の実施の形態】本発明の個人情報統合管理システムの実施の形態の一構成例について、図１を用いて説明する。

【００２８】図１において、１０はＩＣカード、２０はＩＣカードサービス端末（以下、カード端末と略す）、３０は複数の通常のＩＣカードサービスシステム（以下、サービスシステムと略す）、４０は個人情報管理システム、５０はネットワークである。

【００２９】本発明の個人情報統合管理システムでは、カード端末２０と、複数のサービスシステム３０と、個人情報管理システム４０とがネットワーク５０を介して接続されている。これらに加え、各ユーザのＩＣカード１０が、単体では機能しないが、カード端末２０のＩＣカードリーダライタ（ＩＣカードＲＷ）２１に挿入されることでシステムの一部として動作する。

【００３０】更に、システムには、ユーザが初めてＩＣカードサービス環境である個人情報統合管理システムにアクセスしようとする際に、該ユーザに初期情報を記録したＩＣカードを発行する個人情報登録システムが接続されていても良い。本発明ではこの個人情報登録システムを必須の構成要素とはしないが、個人情報統合管理システムの中で絶対の信頼機関として個人情報登録システムを使用する構成も可能である。

【００３１】これら個人情報統合管理システムを構成する各構成要素が格納・管理している情報を図２に示す。項目に記した具体的なプロパティは、情報のカテゴリを分かり易く示すための例である。尚、図２において、ハッチングが施してある部分は情報が原本であることを意味している。ここでいう原本とは、各構成要素が主体となって管理する、つまり優先的に扱う情報という意味で

考えて良い。また、ＩＣカードは記憶容量に制限があるので、カード用管理アプリケーションプログラム（ＡＰ）で蓄積するデータはポインタとして機能する情報であっても良い。

【００３２】ＩＣカード１０にはユーザの個人情報が格納されている。個人情報には、ユーザを特定する又はユーザを特徴づけるための住所、氏名、年齢、性別、趣味、嗜好……といった情報等の基本情報と、各サービスシステムのアプリケーションを利用する際に必要なＡＰ個人情報と、個人情報管理システム及び各サービスシステムを介して利用してきたログ情報である個人履歴情報と、そして、これら基本情報・ＡＰ個人情報・個人履歴情報の個々の項目についての利用条件を定めた利用条件情報とがある。

【００３３】サービスシステム３０には、サービスシステム情報と、顧客情報と、ＡＰ個人情報とが格納されている。サービスシステム情報は、該サービスシステムが主体となって管理する、サービスシステムを特定・識別する又はサービスシステムの特徴を示す情報である。顧客情報は、該サービスシステムが主体となって管理する、サービスシステム利用ユーザ毎に取得した情報である。ＡＰ個人情報は、ＩＣカード１０に格納しているＡＰ個人情報の中で、ユーザがサービスシステムに利用を許可している情報であり、ユーザ数の分だけ存在する。

【００３４】個人情報管理システム４０では、ユーザが主体となって管理している、ＩＣカードに格納する個人情報の全て又は個人情報に課せられた利用条件情報が個人情報管理システムに許す範囲の個人情報を格納している。加えて、サービスシステムが主体となって管理しているサービスシステム情報を、各サービスシステムの分だけ管理している。

【００３５】個人情報統合管理システムを利用しようとするユーザは、ユーザ自身の個人情報を管理するために、個人情報管理システム４０の個人情報管理サービス（管理サービス）を使用する。ＩＣカード情報を可視化し、情報を操作するソフトウェアがあれば管理はできるが、ＩＣカード情報をオンラインで扱うためには、個人情報管理システムが必要になる。

【００３６】個人情報管理サービスの概要を図３及び図４を用いて説明する。

【００３７】図３は個人情報管理システムの概要を示すもので、図中、４１は個人情報データベース、４２はサービスシステムデータベース、４３は個人情報管理モジュール、４４はサービスシステム管理モジュール、４５は利用制御モジュールである。また、図４は個人情報管理サービスの処理の流れを示す。

【００３８】初めて個人情報管理システム４０にアクセスするユーザは、予めカード端末２０でＩＣカード１０にカード用個人情報管理ＡＰ（以下、カード用管理ＡＰと略す）１１をダウンロードする。そして、管理サービスを利用する場合、ユーザはカード端末２０で端末用個人情報管理ＡＰ（以下、端末用管理ＡＰと略す）２２を起動し、カード端末２０のＩＣカードＲＷ２１に挿入したＩＣカード１０上のカード用管理ＡＰ１１を用いて、個人情報及び各個人情報に対する利用条件の設定など、個人情報管理の操作を行う。

【００３９】ユーザは、管理サービスを利用して設定した個人情報及び利用条件情報の原本を、ＩＣカード１０上のカード用管理ＡＰ１１に保存する。個人情報管理システム４０の個人情報管理モジュール４３では、カード用管理ＡＰ１１の個人情報と利用条件情報を、管理システム４０に対し定めた利用条件の範囲で個人情報管理システム４０の個人情報ＤＢ４１に保存する。個人情報管理システム４０に対して定める個人情報の利用条件としては、個人情報の全てを取り扱うことができるように特権システムとして定めることが望ましいが、必要ならば適当な利用条件を定めることで利用制御させることも可能である。

【００４０】尚、個人情報管理システム４０中、サービスシステムＤＢ４２、サービスシステム管理モジュール４４及び利用制御モジュール４５については、図７，８を用いて後ほど説明することとし、管理サービスの処理の流れを説明する。

【００４１】カード端末２０で端末用管理ＡＰ２２を起動しておき、そこにＩＣカード１０が挿入されるとＩＣカード１０上のカード用管理ＡＰ１１が起動され、管理サービスが可能になる。カード用管理ＡＰ１１は、本管理サービスのサービス認証を行い、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【００４２】一方、個人情報管理システム４０の個人情報管理モジュール４３は、ＩＣカード利用者のユーザ認証を行い、システム上の個人情報ＤＢ４１から利用条件を判断しながら個人情報の読み出しを行う。これらの個人情報は端末用管理ＡＰ２２に送信され、具体的なユーザの管理操作を受け付ける管理サービスが提供される。

【００４３】ユーザがカード端末２０で個人情報操作の管理サービス処理を行うと、処理内容に応じ、ＩＣカード１０または個人情報管理システム４０に処理内容が送信、処理される。処理が終わればカード端末２０に処理完了の通知が返り、ＩＣカード１０上のカード用管理ＡＰ１１が終了し、カード端末２０での操作に従い、ＩＣカード１０が排出される。

【００４４】次に、サービスシステムによる提供サービスの概要を図５及び図６を用いて説明する。

【００４５】図５はサービスシステムの概要を示すもので、図中、３１はサービスシステム顧客データベース、３２はサービス処理モジュールである。また、図６はサービスシステムにおける提供サービスの処理の流れを示す。

【００４６】初めてサービスシステム３０にアクセスするユーザは、カード用管理ＡＰ１１に加え、カード用サービスＡＰ１２をＩＣカード１０に搭載しておく必要があり、予めカード端末２０で該サービスのカード用サービスＡＰ１２をＩＣカード１０にダウンロードしておく。

【００４７】サービスシステム３０のサービスを受けるには、カード端末２０で端末用サービスＡＰ２３を起動する。この時、既にＩＣカード１０に搭載されているカード用管理ＡＰ１１で保存している個人情報が、サービスに対し定められた利用条件情報の下で利用可能になる。端末用サービスＡＰ２３は、必要に応じてＩＣカード１０上のカード用サービスＡＰ１２及びカード用管理ＡＰ１１と連携して、必要な個人情報を該サービスに課せられた利用条件情報に基づき利用しつつ、該サービスのサービス処理を遂行する。

【００４８】サービスシステム３０では、サービス処理モジュール３２を介し、カード用管理ＡＰ１１によって利用制御された個人情報を用いてサービス処理が行われ、サービスシステム３０が自身で収集したユーザ情報を顧客情報として収集する。

【００４９】サービスシステム３０の処理の流れとしては、まず、カード端末２０で端末用サービスＡＰ２３を起動しておき、そこにＩＣカード１０を挿入する。サービスシステム３０では、ＩＣカード利用者のユーザ認証を行い、サービスシステム３０に格納されているサービスシステム情報を読み出す。ＩＣカード１０では、カード用サービスＡＰ１２の前にカード用管理ＡＰ１１が起動される。カード用管理ＡＰ１１はサービスシステム情報を参照し、利用しようとしているサービスシステム３０の認証を行う。そして、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【００５０】ＩＣカード１０上で動作するＡＰの制約から、ＡＰの複数起動が可能な場合と不可能な場合とがある。図６の例では、カード用管理ＡＰ１１とカード用サービスＡＰ１２の双方のＡＰが同時に起動しないと仮定して、カード用管理ＡＰ１１を終了させた後、カード用サービスＡＰ１２を起動している。

【００５１】カード用サービスＡＰ１２の起動を受けて、端末用サービスＡＰ１１はＩＣカード１０からサービスに用いる情報の読み出しを行い、また、サービスシステム３０からは顧客ＤＢ３１から顧客情報の読み出しを行う。これらの情報は端末用サービスＡＰ２３に送信され、具体的なユーザの操作を受け付けるサービス提供が開始される。ユーザがカード端末２０でサービス操作を行うと、処理内容に応じ、ＩＣカード１０またはサービスシステム３０に処理内容が送信、処理される。

【００５２】ＩＣカード１０とサービスシステム３０での各々の処理の結果、必要に応じてＩＣカード１０または顧客ＤＢ３１に処理情報の書き込みが行われる。例えば、売買に関するサービスが行われた場合を考えると、売買情報はサービスシステム３０の顧客ＤＢに書き込まれるだけでなく、ユーザの要求に基づき、カード端末２０を介してＩＣカード１０にも送信される。ＩＣカード１０では、サービスシステム毎にフォーマットが異なる前記情報を、カード用管理ＡＰ１１が適当な統一フォーマットの個人履歴情報に変換して該ＩＣカード１０内に格納する。

【００５３】サービスに関する一連の処理が終わればカード端末２０に処理完了の通知が返り、ＩＣカード１０上のカード用サービスＡＰ１２が終了し、カード端末２０での操作に従い、ＩＣカード１０が排出される。

【００５４】次に、個人情報管理システムの個人情報ＤＢとサービスシステムの顧客情報ＤＢとを連携させるサービスについて図７及び図８を用いて説明する。図７は個人情報管理システム及びサービスシステムの概要を示す。また、図８は連携サービスの処理の流れを示す。

【００５５】サービスシステム３０は、ＩＣカード１０との接続を必要としない処理が目的で個人情報を扱おうとする場合や、統計処理などユーザ一般に関する情報を用いた処理を行う場合等に、個人情報管理システム４０の管理サービスを利用する。サービスシステム３０の顧客情報と個人情報管理システム４０の個人情報を連携させるには、各データベースにユーザを特定するためのキーを設定しておく。この方法の詳細は図９を用いて別途説明する。

【００５６】さて、個人情報管理システム４０の個人情報管理サービスを利用するサービスシステム３０は、個人情報管理システム４０のサービスシステム管理モジュール４４を介し、サービスシステムＤＢ４２にサービスシステム情報を登録しておく必要がある。サービスシステム情報の具体的な項目としては、サービスシステム毎に振られたサービスシステムＩＤ、サービスシステムの正当性を認証するための情報、サービスシステムの提供するサービスのカテゴリや特徴的キーワード等が挙げられる。

【００５７】個人情報管理システム４０は、サービスシステム３０の要求に対しサービスシステム管理モジュール４４でサービスシステムとしての認証等の処理を行い、利用制御モジュール４５で該サービスシステム３０の利用条件を判断し、許された範囲内で個人情報ＤＢ４１から個人情報を抽出し、該個人情報をサービスシステム３０に送信する。あるいは定められた利用条件によっては、逆に個人情報管理システム４０で該情報を用いた処理を行い、許可された結果のみをサービスシステム３０に送信する。

【００５８】個人情報管理システムとサービスシステムとの情報連携処理の流れとしては、まず、サービスシステム３０から個人情報管理システム４０へ、管理サービ

ス利用のためのアクセス要求が送信される。管理システム４０はアクセス要求したサービスシステム３０の認証を行い、サービスシステムＤＢ４２からサービスシステム情報の読み出しを行う。

【００５９】サービスシステム３０は、更に、サービスシステム３０で得られている顧客情報と個人情報に基づき、管理サービスの個人情報利用要求を送信する。すると管理システム４０は、サービスシステム３０の顧客ＩＤに対応するユーザＩＤの個人情報との関連付けを行う。関連付けの方法は、先にも述べたように後述する。管理システム４０は、関連付けられた個人情報を個人情報ＤＢ４１から読み出し、該個人情報の利用条件を解析し、利用条件付き個人情報を生成する。サービスシステム３０は、自ら所有する顧客情報に利用条件を設定して、これを管理システム４０に送付する。

【００６０】この時点で個人情報管理システム４０にユーザに関する各種情報が取り揃えられたことになるが、個人情報管理システム４０では、利用制御モジュール４５において、個人情報と顧客情報を連携させ、連携情報に対しどのような利用条件情報を付与すれば良いかの解析を行う。そして、その判断に基づき、利用条件付きの連携情報が生成され、管理サービスの処理結果としてサービスシステム３０に利用条件付き連携情報を引き渡す。

【００６１】以上が一連の処理の流れであるが、利用条件に依っては、最後の工程で連携情報がサービスシステム３０に引き渡されず、個人情報管理システム４０上でのみ取り扱い可能な状態になることもある。このような時、もしもサービスシステム３０に連携情報入手の許可は無くても、連携情報を使った別の処理が許可されていれば、個人情報管理システム４０の利用制御モシュール４５において処理が行われ、サービスシステム３０に処理結果を返送することになる。

【００６２】次に、ＩＣカード１０から個人情報管理システム４０に送信され格納されている個人情報とサービスシステム３０に格納されている顧客情報との連携サービスの実現例を図９を用いて説明する。ここでは、不必要な個人情報の公開を防ぐため、匿名性を維持しつつ顧客情報に対応する連携先個人情報を判断する方法を例示する。

【００６３】個人情報管理システム４０には、ＩＣカード１０の個人情報が、ユーザが設定した利用条件と共に格納されている（ステップ１－１）。これに加え、ＩＣカード１０または個人情報管理システム４０で暗号鍵と復号鍵のペアを作成し、鍵ＩＤを付与しておく。そして、ＩＣカード１０に暗号鍵と鍵ＩＤを格納し、また、個人情報管理システム４０の復号鍵ＤＢ４６に復号鍵と鍵ＩＤを格納しておく（ステップ１－２）。

【００６４】ＩＣカード１０では、ユーザＩＤを暗号鍵で暗号化した暗号化ユーザＩＤ（暗号化ＵＩＤ）を生成する（ステップ１－３）。ユーザがサービスシステム３０のサービスを受ける際には、該暗号化ＵＩＤと鍵ＩＤをサービスシステム３０に送信し（ステップ２－１）、サービスシステム３０は顧客情報を入手する（ステップ２－２）。

【００６５】サービスシステム３０は、ユーザがサービスを利用する際にユーザから取得した顧客情報を、個人情報管理システム４０の個人情報と連携させるために、まず、サービスシステム３０から個人情報管理システム４０に暗号化ＵＩＤと鍵ＩＤとを送信する（ステップ３－１）。

【００６６】個人情報管理システム４０では、鍵ＩＤを基に復号鍵ＤＢを検索し、鍵ＩＤに該当する復号鍵で暗号化ＵＩＤを復号し、ユーザＩＤを特定する（ステップ３－２）。得られたユーザＩＤを基に個人情報ＤＢ４１を検索し、顧客情報と連携させるべき個人情報を得る（ステップ３－３）。

【００６７】個人情報管理システム４０の利用制御モジュール４５は、サービスシステム３０に許可された利用条件を判断し、サービスシステム３０に提供を許された情報については利用制御を課したまま、個人情報管理システム４０からサービスシステム３０に送信する。サービスシステム３０への該個人情報の提供は許されていないが、顧客情報と個人情報とを用いて行う何らかの処理の結果を知ることが許可されている場合、サービスシステム３０から個人情報管理システム４０へ該顧客情報を送信し、個人情報と連携させて実行した処理結果をサービスシステム３０に返送する。

【００６８】サービスシステム３０が、個人情報の提供も個人情報を用いた処理の実行も許されていない場合、サービスシステム３０から個人情報管理システム４０への情報連携要求は不成功に終わる。

【００６９】情報連携を用いた具体的な実施サービス例として、また、本発明の個人情報統合管理システムの発展的サービス例として、サービスシステムが顧客情報と個人情報との連携情報を統計情報として顧客動向調査に利用し、抽出した個人に対し広告を配送するサービスについて述べる。

【００７０】あるサービスシステム（例えば、ＳＳ－Ａとする）の顧客情報ＤＢにサービス履歴情報を蓄積しておく。仮に、ＳＳ－Ａが、ＳＳ－Ａの提供するサービス甲を受けた顧客に特徴的な傾向を発見したとする。ＳＳ－Ａは個人情報管理システム４０と連携して、前記の特徴的な傾向を見せた顧客の顧客ＩＤと、情報から関連付けられたユーザの個人情報を統計的に提供してもらう。

【００７１】この時のユーザの利用条件では、例えば「母数１００以上の統計処理への利用を許可」等の設定がなされている必要があり、そのような提供を許可していないユーザの個人情報は、統計情報としても提供されない。ＳＳ－Ａは、情報連携で得られた統計情報の分析

の結果、例えば「サービス甲を受け、引き続きサービス乙を利用する顧客は２０代女性に多数見られる」等のマーケティング情報を得ることができる。

【００７２】上記マーケティング情報を得たＳＳ－Ａは、サービス甲の利用ユーザの中でまだサービス乙を利用していない顧客に何らかの働きかけを行う、または広く一般ユーザに対して働きかけを行うと考えられる。その働きかけの手段として広告配送による方法がある。しかし、広告配送先である住所情報は、個人情報の１項目であり、ＳＳ－Ａに公開されるとは限らない。そこで、信用できる機関が広告配送サービスを行う仲介することが考えられる。

【００７３】図９における説明では、個人情報管理システムを信用できる機関として、個人情報管理システムで情報連携を行う例を記した。しかし、広告配送専用のサービスシステムＢ（例えば、ＳＳ－Ｂ）が信用できるか、またはＳＳ－Ｂが利用条件を課せられた上でサービスを提供するならば、情報連携をＳＳ－Ｂで行う方法も採ることができる。実現には、暗号・認証技術と、カプセル化等を用いた利用制御技術を用いた方法が考えられる。

【００７４】ＳＳ－Ｂが該サービスを提供する場合、ＳＳ－Ａは広告情報をカプセル化し、広告情報の内容だけでなくＳＳ－Ａが発信者であることも掌握できないような利用条件と共にＳＳ－Ｂに送り、ＳＳ－Ｂは対応するユーザの個人情報から住所（電子メール広告の場合はメールアドレス）を調べ、関連付けることだけが可能な利用条件を課せられているが、該ユーザのもとに広告情報を配送することは実現できる。

【００７５】

【発明の効果】以上述べたように、本発明では、複数のサービスシステムが構築されると、ユーザの個人情報が複数のサービスシステムで独立に存在し、各サービスシステムで管理されることになるところを、個人情報を各サービスシステムで統一的に管理するための個人情報管理システムを設けることで、個人情報の一元的な管理を共通のサービス環境で実現している。

【００７６】これにより、ユーザは１枚のＩＣカードで複数のサービスシステムを利用できるようになり、また、ユーザがその個人情報をユーザ自身で管理することが可能になり、また、ユーザの個人情報を１度更新するだけで各サービスシステムに行き届かせることができる。そして、ユーザ自身の個人情報にユーザ自身が利用条件を課することで、個人情報管理システムに保存した個人情報がどのように利用されているかを情報収集することが可能になる。

【００７７】サービス提供者にとっては、本発明により、従来収集していた顧客の個人情報がサービスシステムの顧客情報ＤＢに格納できなくなるという弊害がある。しかし、顧客情報管理に要する余分な設備投資や運用稼動を必要としないため、コストを抑えることができる。また、個人情報管理主体がユーザに戻ったことで、個人情報の信頼度が高まり、サービスシステム側で個人情報管理責任を負わなくて良いという効果がある。

【００７８】更に、顧客情報と個人情報を連携する仕組みをユーザの個人情報の匿名性に留意しつつ実現することで、従来の機能、即ちユーザが要望としている広告情報等のサービスに関する情報を入手する機能と、サービスシステムが要望している個人情報を用いたマーケティング情報を入手する機能とを維持することができる。

【図面の簡単な説明】

【図１】本発明の個人情報統合管理システムの実施の形態の一例を示す構成図

【図２】本システムの各構成要素に格納される個人情報の具体例を示す説明図

【図３】個人情報管理システムの概要を示す構成図

【図４】個人情報管理サービスの処理の流れ図

【図５】サービスシステムの概要を示す構成図

【図６】サービスシステムにおける提供サービスの処理の流れ図

【図７】個人情報管理システム及びサービスシステムの概要を示す構成図

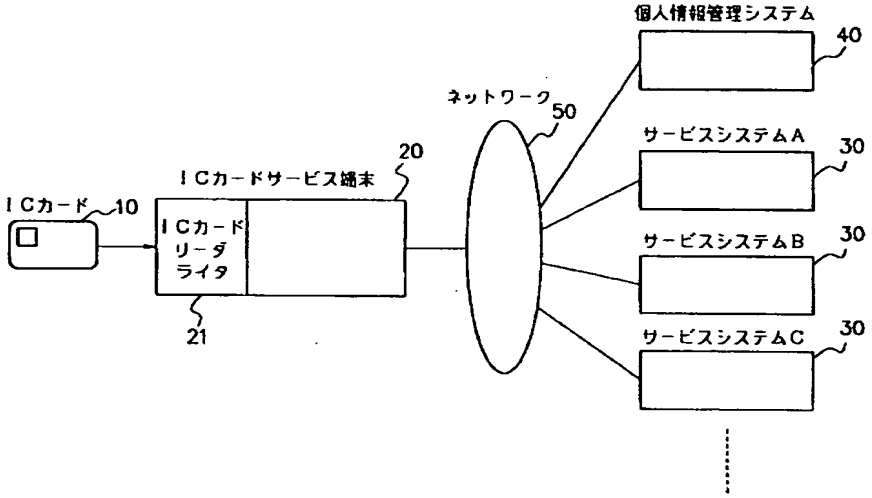
【図８】個人情報管理システムとサービスシステムとの連携サービスの処理の流れ図

【図９】連携サービスの実現例を示す説明図

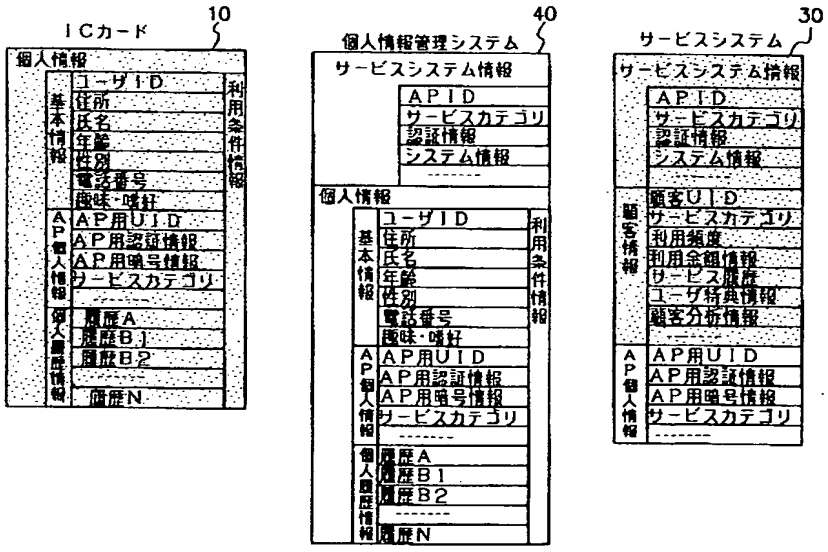
【符号の説明】

１０：ＩＣカード、１１：カード用管理ＡＰ、１２：カード用サービスＡＰ、２０：ＩＣカードサービス端末、２１：ＩＣカードＲＷ、２２：端末用管理ＡＰ、２３：端末用サービスＡＰ、３０：サービスシステム、３１：サービスシステム顧客ＤＢ、３２：サービス処理モジュール、４０：個人情報管理システム、４１：個人情報ＤＢ、４２：サービスシステムＤＢ、４３：個人情報管理モジュール、４４：サービスシステム管理モジュール、４５：利用制御モジュール、５０：ネットワーク。

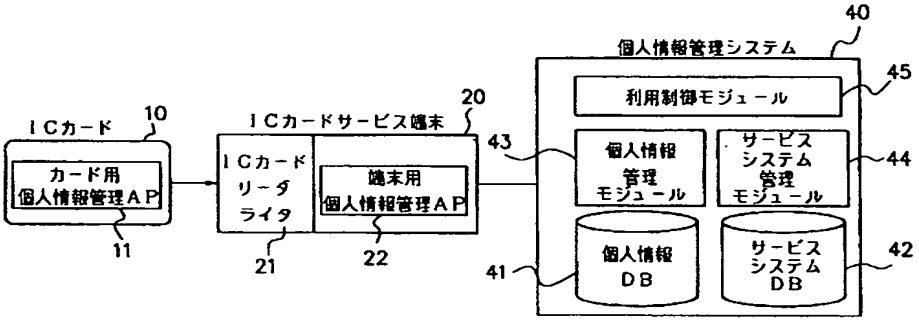
【図1】


個人情報管理システム
40
ネットワーク
50
サービスシステムA
30
20
ICカードサービス端末
ICカード
10
ICカード
リーダ
ライタ
サービスシステムB
30
21
サービスシステムC
30

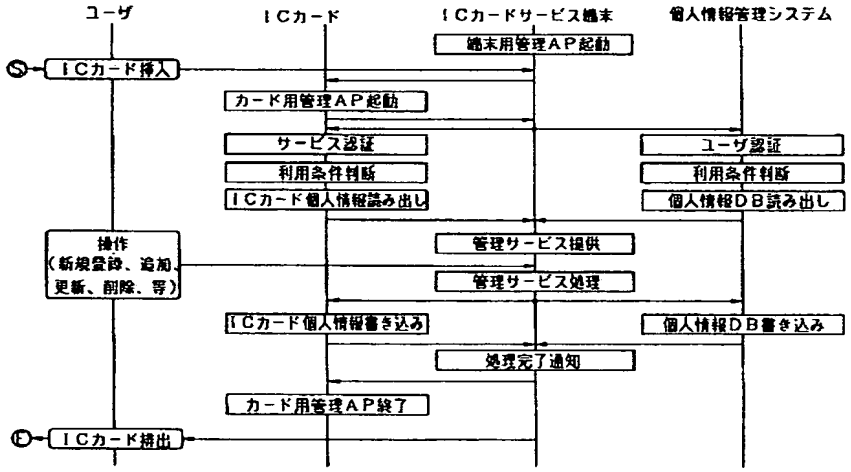
【図2】


ICカード
10
個人情報
基本情報
ユーザID
住所
氏名
年齢
性別
電話番号
趣味・嗜好
AP個人情報
AP用UID
AP用認証情報
AP用暗号情報
サービスカテゴリ
個人履歴情報
履歴A
履歴B1
履歴B2
履歴N
利用条件情報
個人情報管理システム
40
サービスシステム情報
APID
サービスカテゴリ
認証情報
システム情報
サービスシステム
30
顧客情報
顧客UID
利用頻度
利用金額情報
サービス履歴
ユーザ特典情報
顧客分析情報

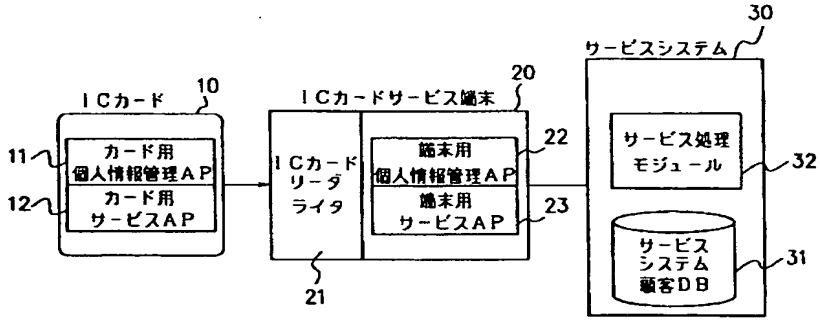
【図3】


40
個人情報管理システム
45
利用制御モジュール
ICカード
10
ICカードサービス端末
20
43
個人情報管理モジュール
サービスシステム管理モジュール
44
カード用個人情報管理AP
ICカードリーダライタ
端末用個人情報管理AP
11
21
22
41
個人情報DB
サービスシステムDB
42

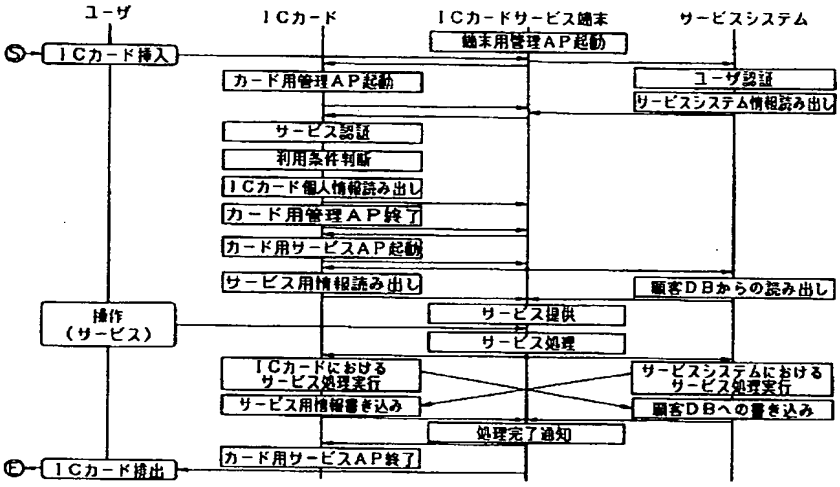
【図4】


ユーザ
ICカード
ICカードサービス端末
個人情報管理システム
端末用管理AP起動
ICカード挿入
カード用管理AP起動
サービス認証
ユーザ認証
利用条件判断
利用条件判断
ICカード個人情報読み出し
個人情報DB読み出し
操作
（新規登録、追加、更新、削除、等）
管理サービス提供
管理サービス処理
ICカード個人情報書き込み
個人情報DB書き込み
処理完了通知
カード用管理AP終了
ICカード排出

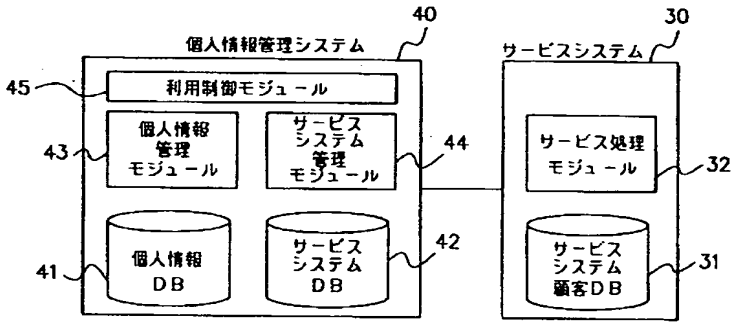
【図5】


30
サービスシステム
ICカード
10
ICカードサービス端末
20
11
カード用個人情報管理AP
12
カード用サービスAP
ICカードリーダライタ
端末用個人情報管理AP
22
端末用サービスAP
23
サービス処理モジュール
32
サービスシステム顧客DB
31
21

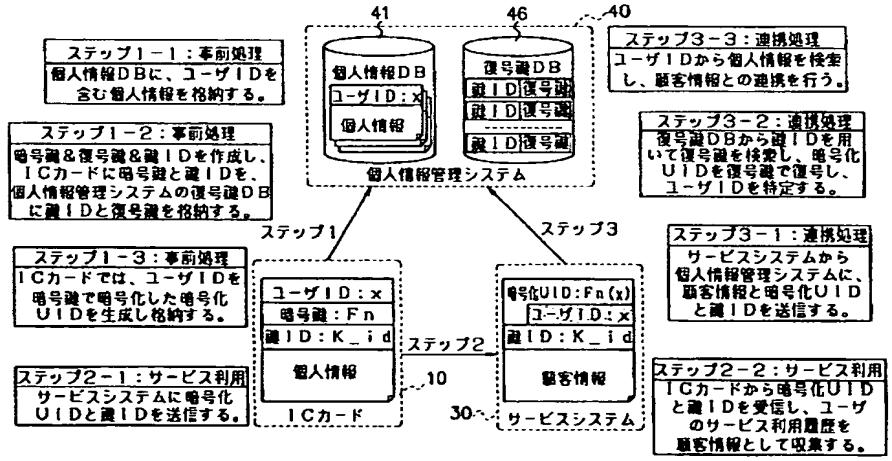
【図6】


ユーザ
ICカード
ICカードサービス端末
サービスシステム
端末用管理AP起動
ICカード挿入
カード用管理AP起動
ユーザ認証
サービスシステム情報読み出し
サービス認証
利用条件判断
ICカード個人情報読み出し
カード用管理AP終了
カード用サービスAP起動
サービス用情報読み出し
顧客DBからの読み出し
操作
（サービス）
サービス提供
サービス処理
ICカードにおける
サービス処理実行
サービスシステムにおける
サービス処理実行
サービス用情報書き込み
顧客DBへの書き込み
処理完了通知
カード用サービスAP終了
ICカード排出

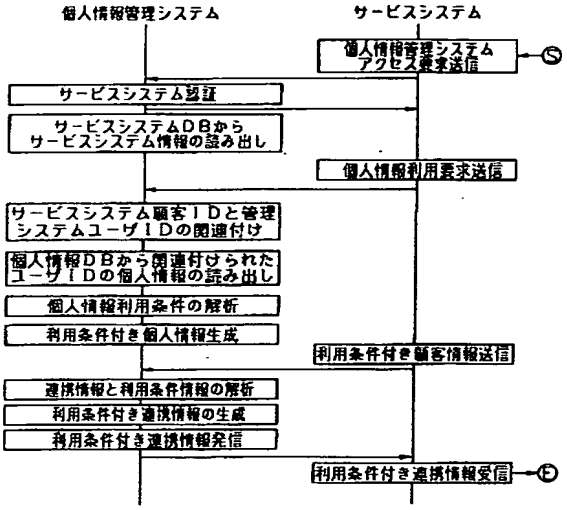
【図7】


40
30
個人情報管理システム
サービスシステム
45
利用制御モジュール
43
個人情報
管理
モジュール
サービス
システム
管理
モジュール
44
サービス処理
モジュール
32
41
個人情報
DB
サービス
システム
DB
42
サービス
システム
顧客DB
31

【図9】


41
46
40
ステップ1－1：事前処理
個人情報DBに、ユーザIDを含む個人情報を格納する。
個人情報DB
ユーザID：x
個人情報
復号鍵DB
鍵ID
復号鍵
ステップ3－3：連携処理
ユーザIDから個人情報を検索し、顧客情報との連携を行う。
ステップ1－2：事前処理
暗号鍵&復号鍵&鍵IDを作成し、ICカードに暗号鍵と鍵IDを、個人情報管理システムの復号鍵DBに鍵IDと復号鍵を格納する。
ステップ3－2：連携処理
復号鍵DBから鍵IDを用いて復号鍵を検索し、暗号化UIDを復号鍵で復号し、ユーザIDを特定する。
個人情報管理システム
ステップ1
ステップ3
ステップ1－3：事前処理
ICカードでは、ユーザIDを暗号鍵で暗号化した暗号化UIDを生成し格納する。
ステップ3－1：連携処理
サービスシステムから個人情報管理システムに、顧客情報と暗号化UIDと鍵IDを送信する。
ユーザID：x
暗号鍵：Fn
鍵ID：K_id
個人情報
ステップ2
暗号化UID：Fn(x)
ユーザID：x
鍵ID：K_id
顧客情報
ステップ2－1：サービス利用
サービスシステムに暗号化UIDと鍵IDを送信する。
10
ICカード
30
サービスシステム
ステップ2－2：サービス利用
ICカードから暗号化UIDと鍵IDを受信し、ユーザのサービス利用履歴を顧客情報として収集する。

【図8】



フロントページの続き

(72)発明者　林　良一
東京都千代田区大手町二丁目３番１号　日
本電信電話株式会社内